Advanced Security 1 - CMPU4007
Week 3 - Block Ciphers DES

In this lab you are required to provide solutions to the questions below.

DES cipher in ECB mode

Q 1. Write a program to encrypt and decrypt the following with the DES cipher in ECB mode:
Key: 12345678
Plaintext: AAAABBBBAAAABBBB
Ciphertext: 19FF4637BB2FE77C19FF4637BB2FE77C

DES cipher in CBC mode

Q 2. Write a program to encrypt and decrypt the following with the DES cipher in CBC mode:
Key: 12345678
IV: 00000000
Ciphertext: AAAABBBBAAAABBBB
Plaintext: AAC823F6BBE58F9EAF1FE0EB9CA7EB08

Padding

Q 3. Write 2 functions to add and remove padding from ASCII data which will be encrypted using DES in ECB mode.
Key: 12345678
Plaintext: AAAABBBBCCCC
Plaintext with padding: AAAABBBBCCCC\x00\x0004
Ciphertext (base 16 encoded): 19FF4637BB2FE77C81987E5CB99B66E2

Deliverables: Please submit the plaintexts, ciphertexts, keys,code and notes written.

Attached:
FIPS PUB 81 - DES MODES OF OPERATION

The following method may be used for applications where the length of the cipher text can be greater than the length of the plain text. In this case the final partial data block of a message is padded in the least significant bits positions with "0"s, "1"s or pseudo- random bits. The decryptor will have to know when and to what extent padding has occurred. This can be accomplished explicitly, e.g., using a padding indicator, or implicitly, e.g., using constant length transactions. The padding indicator will depend on the data being encrypted.

If the data is pure binary, then the partial data block should be left justified in the input block and the unused bits of the block set to the complement of the last data bit, i.e., if the last data bit of the message is "0" then "1"s are used as padding bits and if the last data bit is"1" then "0"s are used. The input block is then encrypted. The resulting output block is the cipher text. The cipher text message must be marked as being padded so that the decryptor can reverse the padding process, remove the padding bits and produce the original plain text. The decryptor scans the decrypted padded block and discards the least significant bits that are all identical.

If the data consists of bytes (e.g., 8-bit ASCII characters) then the padding indicator should be a character denoting the number of padding bytes, including itself, and should be placed in the least significant byte of the input block before encrypting. For example if there are five ASCII data characters in the final partial block of a message to be encrypted, then an ASCII "3" is put in the least significant byte of the input block (any pad characters may be used in the other two pad positions) before encryption. Again the cipher text message must be marked as being padded.